553,306

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2004 (16.12.2004)

PCT

(10) International Publication Number
WO 2004/109971 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/US2003/016817

(22) International Filing Date: 30 May 2003 (30.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE [US/US]; 9201 University City Boulevard, Charlotte, NC 28223-0001 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: ZHENG, Yuliang [AU/US]; 3122 Bridle Brook Way, Charlotte, NC 28270 (US). TEO, Lawrence, Chin, Shiun [MY/US]; 1225 University Walk Circle, Apt. 102, Charlotte, NC 28213 (US). AHN, Gail-Joon [KR/US]; 7801 Peach Blossom Court, Harrisburg, NC 28075 (US).

(74) Agents: ALEMANNI, John, C. et al.; Kilpatrick Stockton LLP, 1001 West Fourth Street, Winston-Salem, NC 27101 (US).

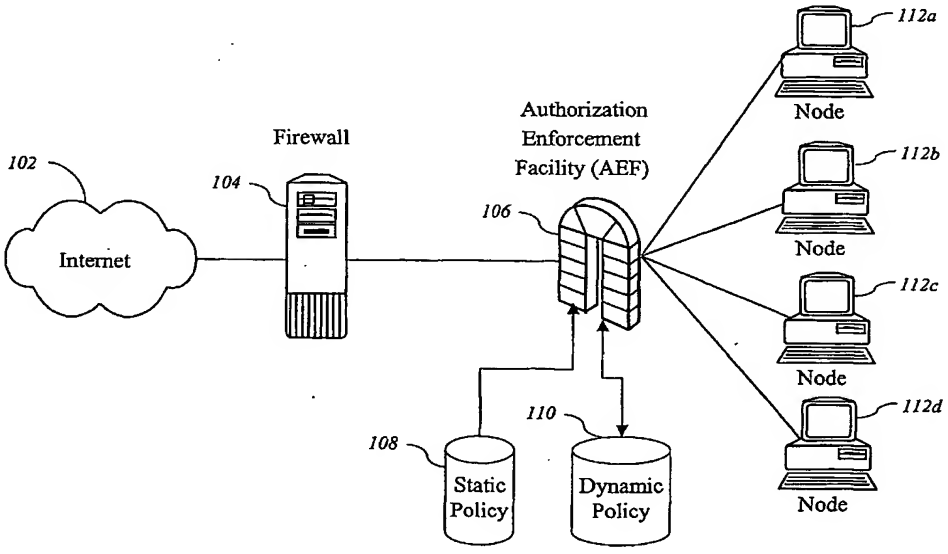
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR DYNAMIC AND RISK-AWARE NETWORK SECURITY



(57) Abstract: Systems and methods for dynamic and risk-aware network security are described. In one embodiment, a system dynamically assesses whether a connection over a communications medium (102) is anomalous (suspicious, malicious, deviating from normal behavior, fits a certain profile or pattern, or has the potential to be any one of these) and generates an appropriate response depending on whether the connection is deemed to be normal or anomalous for a specified period of time. The types of responses include, but are not limited to, blocking the source of the connection from connecting to its intended destination, altering the destination of the connection, auditing the connection, or any combination of these.

WO 2004/109971 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.